FAA- HDBK- 004
September 4, 1997

DEPARTMENT OF TRANSPORTATION

FEDERAL AVIATION ADMINISTRATION

HANDBOOK

NATIONAL AIRSPACE SYSTEM INTERNET PROTOCOL SUITE

AREA SDMP

FOREWORD

This document defines the protocol standards for the Internet Protocol Suite (IPS), which is commonly referred to as Transmission Control Protocol/Internet Protocol (TCP/IP) protocols used for data communications within the National Airspace System (NAS). This handbook is for guidance only. It cannot be cited as a requirement. If it is cited as a requirement, the contractor does not have to comply.

CONTENTS

PARAGRAPH PAGE

1. . . . SCOPE 1
1.1 . . . . Scope 1
1.2 . . . . Purpose 1

2. . . APPLICABLE DOCUMENTS 2
2.1 . . . . Government documents 2
2.2 . . . . Non- Government documents 3
2.3 . . . . Document sources 5
2.3.1 . . . FAA documents 5
2.3.2 . . . Federal or military documents 5
2.3.3 . . . Request for comments 5

3. . . . DEFINITIONS 6
3.1 . . . . . Acronyms 6
3.2 . . . . . Internet 8
3.3 . . . . . Network 8
3.4 . . . . . Profile 8
3.5 . . . . . Protocol 8
3.6 . . . . . Socket 8
3.7 . . . . . Subnetwork 8
3.8 . . . . . Subprofile 8
3.9 . . . . . World Wide Web 8

4. . . . GENERAL RECOMMENDATIONS 9
4.1 . . . . Link layer subprofile 10
4.2 . . . . Network layer subprofile 11
4.3 . . . . Transport layer subprofile 11
4.4 . . . . Application layer subprofile 11

5. . . DETAILED RECOMMENDATIONS 11
5.1 . . . . User profiles 11
5.1.1 . . . Link subprofile 12
5.1.1.1 . LAN connections 13
5.1.1.1.1 Ethernet 13
5.1.1.1.2 IEEE 802 13
5.1.1.1.3 FDDI 13
5.1.1.1.4 ARP/Reverse Address Resolution Protocol (RARP) 13
5.1.1.2 . Serial interfaces 13

CONTENTS

PARAGRAPH PAGE

5.1.1.3 . Packet Switched Network (PSN X.25) 13
5.1.1.4 . Loopback interface 14
5.1.1.5 . Maximum Transmission Unit (MTU) 14
5.1.2 . . . Network subprofile 14
5.1.2.1 . Internet Protocol (IP) 14
5.1.2.1.1 Network addressing 14
5.1.2.1.2 Subnet extensions 14
5.1.2.1.3 IP multicasting 14
5.1.2.2 . Routing 14
5.1.2.2.1 IGP 14
5.1.2.2.2 EGP 15
5.1.2.2.3 Error detection and reporting 15
5.1.2.3 . Network control protocol for PPP 15
5.1.3 . . . Transport subprofile 15
5.1.3.1 . TCP 15
5.1.3.2 . UDP 15
5.1.4 . . . User extended subprofile 15
5.1.4.1 . . Remote login 16
5.1.4.1.1 Telnet 16
5.1.4.2 . File transfer 16
5.1.4.2.1 FTP 16
5.1.4.2.2 TFTP 16
5.1.4.3 . Electronic mail 16
5.1.4.3.1 SMTP 16
5.1.4.4 . Support services 17
5.1.4.4.1 Domain name system 17
5.1.4.4.2 Host initialization 17
5.1.4.5 . Network management 17
5.1.4.6 . Security 17
5.1.4.7 . Priority 17
5.1.4.8 . Interoperability and conformance testing 17
5.1.4.9 . Naming and addressing 17

6. . . NOTES 18
6.1 . . . . Application program interface 18
6.1.1 . . . Sockets 18

CONTENTS

PARAGRAPH PAGE

FIGURE

1 . . . Internet protocol suite 1
2 . . . Protocol suite 9
3 . . . Internet protocol suite, protocol stack 12
4 . . . Subprofile layers 12

APPENDIX

A PROFILE RECOMMENDATIONS LISTS COMMUNICATIONS LAYERS 19
B PROFILE RECOMMENDATIONS LISTS APPLICATION LAYER 30

TABLE

A- I . Link layer conditions summary 20
A- II Internet protocol layer conditions summary 21
A- III UDP conditions summary 26
A- IV TCP conditions summary 27
B- I . General application conditions summary 31
B- II Telnet conditions summary 32
B- III FTP conditions summary 34
B- IV TFTP conditions summary 36
B- V SMTP conditions summary 37
B- VI Domain name system conditions summary 39
B- VII Management conditions summary 41

1. SCOPE

1.1 Scope. This handbook recommends the protocols, features, and services that should be supported in a Federal Aviation Administration (FAA) IPS environment within the National Airspace System (NAS). This handbook will focus on documenting the required TCP/IP standards for connection oriented service and User Datagram Protocol (UDP) standards for connectionless service, see Figure 1. This handbook is for guidance only. It cannot be cited as a requirement. If it is, the contractor does not have to comply.

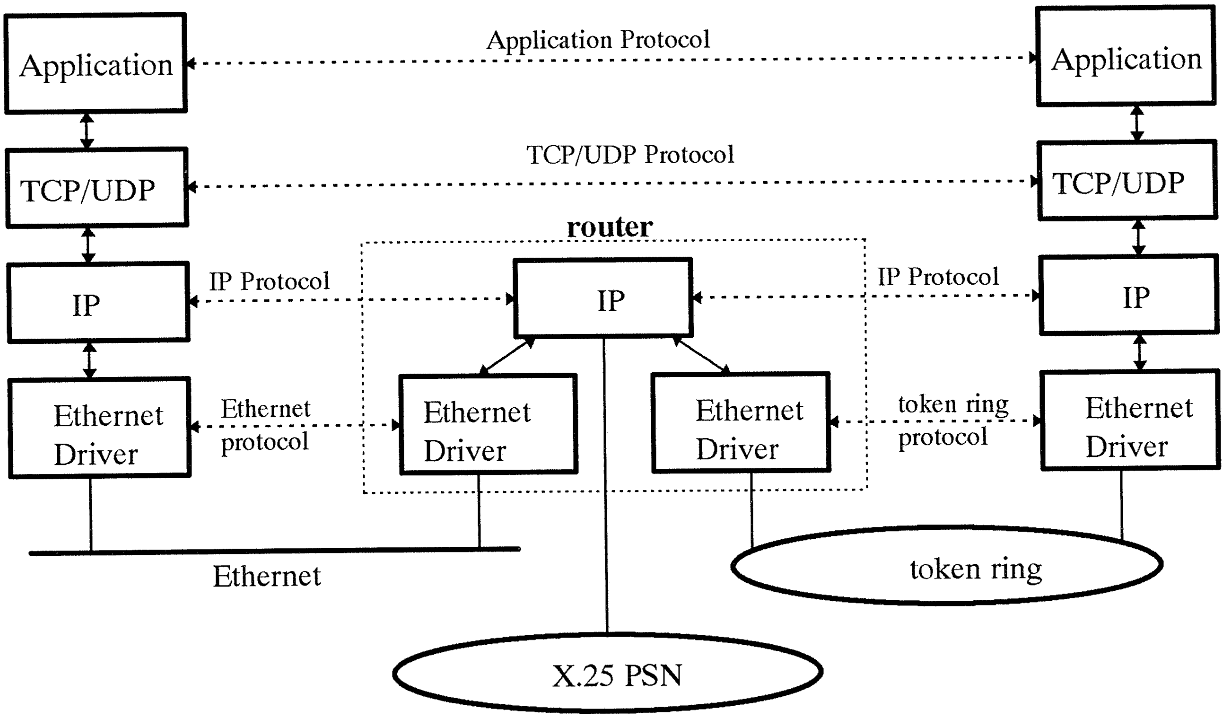

FIGURE 1. Internet protocol suite

Specified in this handbook are the minimum recommendations, additional protocols and services that may be implemented by mutual agreement. The minimum set defined herein may exceed the minimum requirements for a particular subnetwork.

This document was prepared in accordance with FAA-STD-005e.

1.2 Purpose. The purpose of this document is to recommend standardized IPS protocols, options, and service elements that are available for implementation within FAA subnetworks. It will also assist FAA project personnel in determining the minimum features and options that must be supported in order to ensure uniform IPS implementation throughout the FAA. Finally, the implementation of the material presented in this handbook will allow FAA systems to be compatible with the global internet and enable transparent interface with the existing network infrastructure to support current and future FAA programs.

2. APPLICABLE DOCUMENTS

2.1 Government documents. The following government documents form a part of this handbook to the extent specified herein. In the event of conflict between the documents referenced herein and the content of this handbook, the content of this handbook shall be considered the superseding document.

Standards

FAA-STD-005e	Preparation of Specifications, Standards and Handbooks, 1996
FAA-STD-039B	National Airspace System (NAS), Open Systems Architecture and Protocols, 1996
FAA-STD-042A	OSI Naming and Addressing Registration, 1994
FAA-STD-043A	Open System Interconnection (OSI), Priority, 1994
FAA-STD-045	Open System Interconnection (OSI), Security Architecture Protocols and Mechanisms, 1994
FAA-STD-047	Open System Interconnection (OSI), Conformance Testing, 1993
FAA-STD-048	Open System Interconnection (OSI), Interoperability Standard, 1995
FAA-STD-049	Fiber Optic Standard for Telecommunication Systems and Equipment, 1994

Federal Information Processing Standards (FIPS)

FIPS PUB 146-2	Profiles for Open Systems Internetworking Technology (POSIT), 1994

Other Government Publications

FAA-HDBK-002	Systems Management, 1997
ENET1370-002.1A	FAA Enterprise Network, Internet Packet Exchange (IPX) and Transmission Control Protocol/Internet Protocol (TCP/IP) Address Assignments

2.2 Non-Government documents. The following non-government documents form a part of this handbook to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this handbook, the contents of this handbook shall be considered the superseding document.

Internet Standards

RFC-768	User Datagram Protocol, J. Postel, August 1980
RFC-791	Internet Protocol, J. Postel, September 1981
RFC-793	Transmission Control Protocol, J. Postel, September 1981
RFC-821	Simple Mail Transfer Protocol, J. Postel, August 1982
RFC-826	Ethernet Address Resolution Protocol, D. Plummer, November 1982
RFC-854	Telnet Protocol Specification, J. Postel, J.K. Reynolds, May 1983
RFC-894	Standard for the Transmission of IP Datagrams over Ethernet Networks, C. Hornig, April 1984
RFC-903	Reverse Address Resolution Protocol, R. Finlayson, T. Mann, J.C. Mogul, M. Theimer, June 1984
RFC-950	Internet Standard Subnetting Procedure, J. Mogul, J. Postel, August 1985
RFC-951	Bootstrap Protocol, W.J. Croft, J. Gilmore, September 1985
RFC-959	File transfer Protocol, J. Postel, J.K. Reynolds, October 1985
RFC-974	Mail Routing and the Domain System, C. Partridge, January 1986
RFC-1042	Standard for the Transmission of IP Datagrams over 802 Networks, J. Postel, J. Reynolds, February 1988
RFC-1055	Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP, J.L. Romkey, June 1988
RFC-1101	DNS Encoding of Network Names and Other Types, P.V. Mockapetris, April 1989

RFC-1112	Host Extensions for IP Multicasting, S.E. Deering, August 1989
RFC-1122	Requirements for Internet Hosts-Communications Layers, R. Braden, October 1989
RFC-1123	Requirements for Internet Hosts-Application and Support, R. Braden, October 1989
RFC-1144	Compressing TCP/IP Headers for Low-speed Serial Links, V. Jacobson, February 1990
RFC-1148	Mapping between X.400 (1988)/ISO 100021 and RFC-822, S. Kille, March 1990
RFC-1166	Internet Numbers, S. Kirkpatrick, M. Stahl, M. Recker, July 1990
RFC-1183	New DNS RR Definitions, C.F. Everhart, L.A. Mamakos, R. Ullmann, P.V. Mockapetris, October 1990
RFC-1191	Path MTU Discovery, J.C. Mogul, S.E. Deering, November 1990
RFC-1267	Border Gateway Protocol 3 (BGP-3), K. Lougheed, Y. Rekhter, October 1991
RFC-1332	The PPP Internet Protocol Control Protocol (IPCP), G. McGregor, May 1992
RFC-1356	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, A. Malis, D. Robinson, R. Ullmann, August 1992
RFC-1390	Transmission of IP and ARP over FDDI Networks, D. Katz, January 1993
RFC-1247	OSPF Version 2, J. Moy, March 1994
RFC-1661	The Point-to-Point Protocol (PPP), W. Simpson, July 1994
RFC-1700	Assigned Numbers, J. Reynolds, J. Postel, October 1994
RFC-1706	DNS NSAP Resource Records, B. Manning, R. Coletta, October 1994
RFC-1723	RIP Version 2-Carring Additional Information, G. Malkin, November 1994

RFC-1782	TFTP Option Extension, G. Malkin, A. Harkin, March 1995
RFC-1783	TFTP Blocksize Option, G. Malkin, A. Harkin, March 1995
RFC-1784	TFTP Timeout Interval and Transfer Size Option, G. Malkin, A. Harkin, March 1995
RFC-1785	TFTP Option Negotiation Analysis, G. Malkin, A. Harkin, March 1995
RFC-1880	Internet Official Protocol Standards, J. Postel, November 1995

Other Publications

International Civil Aviation Organization (ICAO) Annex 10, Volume III, Part 2, Chapter 3 (ATN) 1996

2.3 Document sources. Obtain copies of the applicable documents or standards by contacting the appropriate organizations.

2.3.1 FAA documents. Copies of FAA specifications, standards, and publications may be obtained from the Contracting Officer, Federal Aviation Administration, 800 Independence Avenue, S.W., Washington, D.C., 20591. Request should clearly identify the desired material by number and date, and state the intended use of the material.

2.3.2 Federal or military documents. Copies of federal or military documents are available from the Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094

2.3.3 Request for comments. Copies of Request for Comments (RFC) may be obtained from DS.INTERNIC.NET via File Transfer Protocol (FTP), Wide Area Information Service (WAIS), and electronic mail.

If FTP is used, RFCs are stored as rfc/rfcnnnn.txt or rfc/rfcnnnn.ps where "nnnn" is the RFC number. Login as "anonymous" and provide your E-Mail address as the password.

If WAIS is used, the local WAIS client or Telnet to DS.INTERNIC.NET can be used. Login as "wais" (no password is required) to access a WAIS client; help information and a tutorial for using WAIS are available online. Search the "rfcs" database to locate the desired rfc.

If electronic mail is used, send a mail message to mailserv@ds.internic.net and include any of the following commands in the message body:

document-by-name rfcnnnn	where "nnnn" is the RFC number; the text version is sent

file/ftp/rfc/rfcnnnn.yyy	where “nnnn” is the RFC number and “yyy” is “txt” or “ps”

3. DEFINITIONS

3.1 Acronyms. The acronyms used in this handbook are defined as follows:

API	Application Programming Interface
ATN	Aeronautical Telecommunication Network
ARP	Address Resolution Protocol
ARPAnet	Advanced Research Projects Agency Network
BGP	Border Gateway Protocol
BOOTP	Boot Strap Protocol
CL	Connection- less
CMIP	Common Management Information Protocol
CO	Connection- oriented
DGRAM	Datagram
DNS	Domain Name System
DOD	Department of Defense
EGP	Exterior Gateway Protocol
FAA	Federal Aviation Administration
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standards Publication
FTP	File Transfer Protocol
GUI	Graphical User Interface
ICAO	International Civil Aviation Organization
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol

IPS	Internet Protocol Suite
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
LAN	Local Area Network
MILNET	Military Network
MTU	Maximum Transmission Unit
NAS	National Airspace System
NSFNet	National Science Foundation Network
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
POSIT	Profiles for Open Systems Internetworking Technologies
PPP	Point-to-Point Protocol
PSN	Packet Switched Network
RARP	Reverse Address Resolution Protocol
RFC	Request for Comments
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SR	Source Route
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLI	Transport Layer Interface
TS	Timestamp
UDP	User Datagram Protocol
WAIS	Wide Area Information Service
WAN	Wide Area Network

3.2 Internet. A three-level hierarchy composed of backbone networks (e.g. Advanced Research Projects Net [ARPAnet], National Science Foundation Net [NSFNet], Military Network [MILNET]) and mid-level network stub networks. These include commercial (.com or .co), university (.ac or .edu), other research networks (.org or .net), and military (.mil) networks. It spans many different physical networks around the world with various protocols including the IP.

3.3 Network. Hardware and software data communication systems.

3.4 Profile. A list of protocols that support the implementation of a service or function in a network.

3.5 Protocol. A set of formal rules describing how to transmit data, especially across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering, and transmission, error detection, and correction of the bit stream. High-level protocols deal with data formatting, including the syntax of messages, the terminal-to-computer dialogue, character sets, sequencing of messages, etc. Many protocols are defined by RFCs or by International Organization for Standardization (ISO) standards.

3.6 Socket. The Berkeley UNIX mechanism for creating a virtual connection between processes. Sockets form the interface between UNIX standard input/output (I/O) and network communication facilities. They are of two types, stream (bi-directional) or datagram (DGRAM) (fixed length destination-addressed messages). The socket library function socket creates a communications end-point or socket and returns a file descriptor with which the socket is accessed. The socket has an associated socket address, consisting of a port number and the local host's network address.

3.7 Subnetwork. A collection of end systems and intermediate systems under the control of a single administrative domain, which uses a single network access protocol.

3.8 Subprofile. A subset of a profile that supports a specific protocol layer in a network application.

3.9 World Wide Web. An internet client-server distributed information retrieval system which originated in the CERN High-Energy Physics laboratories in Geneva, Switzerland.

4. GENERAL RECOMMENDATIONS

This section specifies general recommendations for implementing the IPS protocols within a subnetwork. The IPS allows computers of all sizes, from different vendors, using different operating systems, to exchange data. This data transfer is accomplished via data networks using protocols that perform different functions at different layers of the data exchange. The complete set of protocols necessary for this communication is referred to as a protocol suite. Depicted in Figure 2 is a typical protocol suite; the suite will vary and is dependent upon the implemented network services.

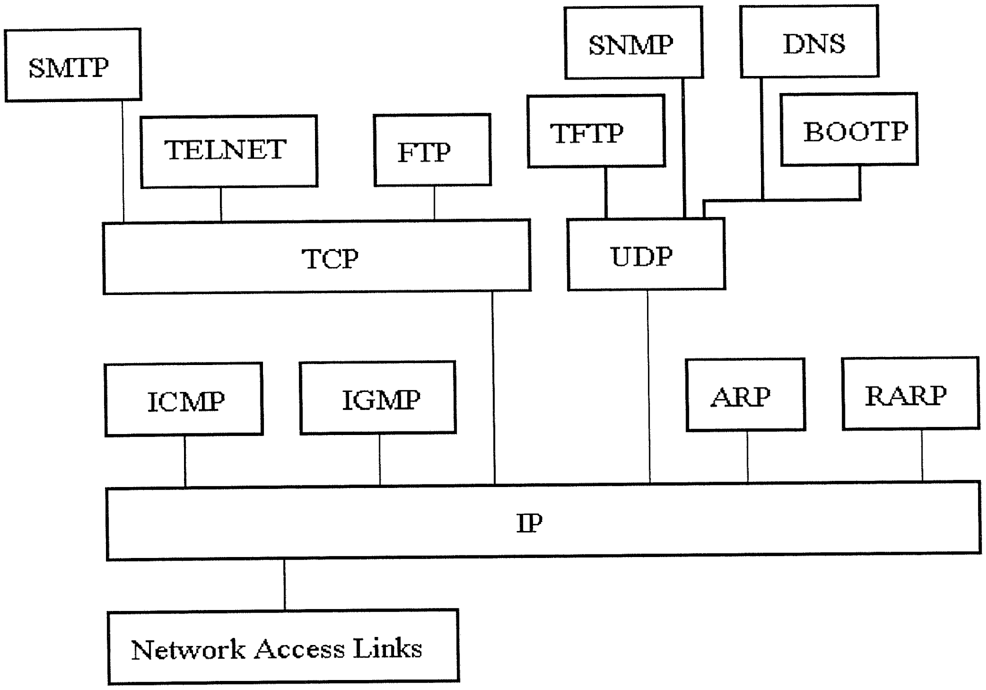

FIGURE 2. Protocol suite

Each layer of the protocol suite supports the implementation of a different function within a communication network. The lower layer will typically provide services to the upper layer by using the services provided by the layer below it. In order to implement the desired network functions, a layer can consist of more than one protocol. The grouping of protocols that support the functional requirements of a protocol layer is referred to as a subprofile.

The link subprofile, also referred to as the network access layer, provides the physical interface to the network and connects the system to the network via the network interface card and device driver. This layer is where the electrical and mechanical characteristics are defined for the network.

The network subprofile, also know as the internet layer, provides for the movement of data packets around the network. This layer handles packet routing, addressing, packet fragmentation, and reassembly and security.

The transport subprofile provides end- to- end communications between two hosts. This layer is used to provide both reliable and unreliable service for an application.

The application subprofile provides the functions and services to an end- user. A few of the services provided are security (remote login), file transfer over the network, and electronic mail delivery.

Implementation of IPS systems that will connect to the Internet systems should be in accordance with RFC- 1880, Internet Official Protocol Standards.

Implementation of the network management system in an IPS network should be in accordance with FAA- HDBK- 002, Systems Management.

The recommendations listed within this handbook comply with Federal Information Publication (FIPS) 146- 2, Profiles for Open Systems Internetworking Technologies (POSIT).

Subnetworks that will interface and support communications with the OSI- based international Aeronautical Telecommunication Network (ATN), must implement the practices and standards contained in the following documents:

- International Civil Aviation Organization (ICAO) Annex 10, Volume III, Part 2, Chapter 3 (ATN);
- National Airspace System Open Systems Architecture and Protocols, FAA- STD- 039B.

4.1 Link layer subprofile. The link layer, or media access layer, normally includes the device drivers for the operating system and the corresponding network interface card installed in the computer. This layer handles the hardware details or the physical interfacing to the transmission medium (i.e., cable, radio link). It provides the mechanical, electrical, functional, and procedural methods necessary to activate, maintain, and deactivate physical connections for data links. General recommendations for implementation of the link layer should be done in accordance with RFC- 1122, Requirements for Internet Hosts- Communication Layer. Detailed recommendations for physical interfaces is contained in Section 5.1.1 of this document, Link Subprofile.

4.2 Network layer subprofile. The network layer handles the movement of packets around the network. This layer performs address conversion between internet protocol addresses and Ethernet addresses in local area network (LAN) environments. This layer also defines the gateway interface, multicast specifications, and low-level network management.

General recommendations for implementation of the network layer should be done in accordance with RFC-1122, Requirements for Internet Hosts-Communication Layer. Detailed recommendations for the network layer are contained in Section 5.1.2 Network subprofile of this document.

4.3 Transport layer subprofile. The transport layer provides a flow of data between two hosts for the application layer above it. In the IPS, there are two vastly different transport protocols: one for reliable connection-oriented service, and the other for unreliable connectionless service. General recommendations for implementation of the transport layer should be done in accordance with RFC-1122, Requirements for Internet Hosts-Communication Layer. Detailed recommendations for the transport layer are contained in Section 5.1.3,Transport subprofile, of this document.

4.4 Application layer subprofile. The application layer handles the details of specific application programs. General recommendations for implementation of the application layer should be done in accordance with RFC-1123, Requirements for Internet Hosts-Application and Support. Detailed recommendations for the application layer are contained in Section 5.1.4, User extended subprofile, of this document.

5. DETAILED RECOMMENDATIONS

This section specifies the detailed recommendations necessary to implement IPS protocols within an FAA subnetwork. Contained in Section 5.1 are the subprofile recommendations that network implementors should follow in order to provide a consistent and uniform data transmission environment within FAA networks. Compliance with these recommendations will allow the same services and features to be supported in all similar networks, enable network-to-network compatibility, standardize maintenance and troubleshooting, and decrease implementation costs.

5.1 User profiles. Networking protocols are typically implemented in a layered approach, with each layer responsible for a different facet of communication. The IPS complies with this philosophy, and consists of various protocols that enable data communications. The complete set of protocol layers is referred to as a protocol stack. The protocols are implemented at different layers of the protocol hierarchy and perform different communication tasks, see Figure 3.

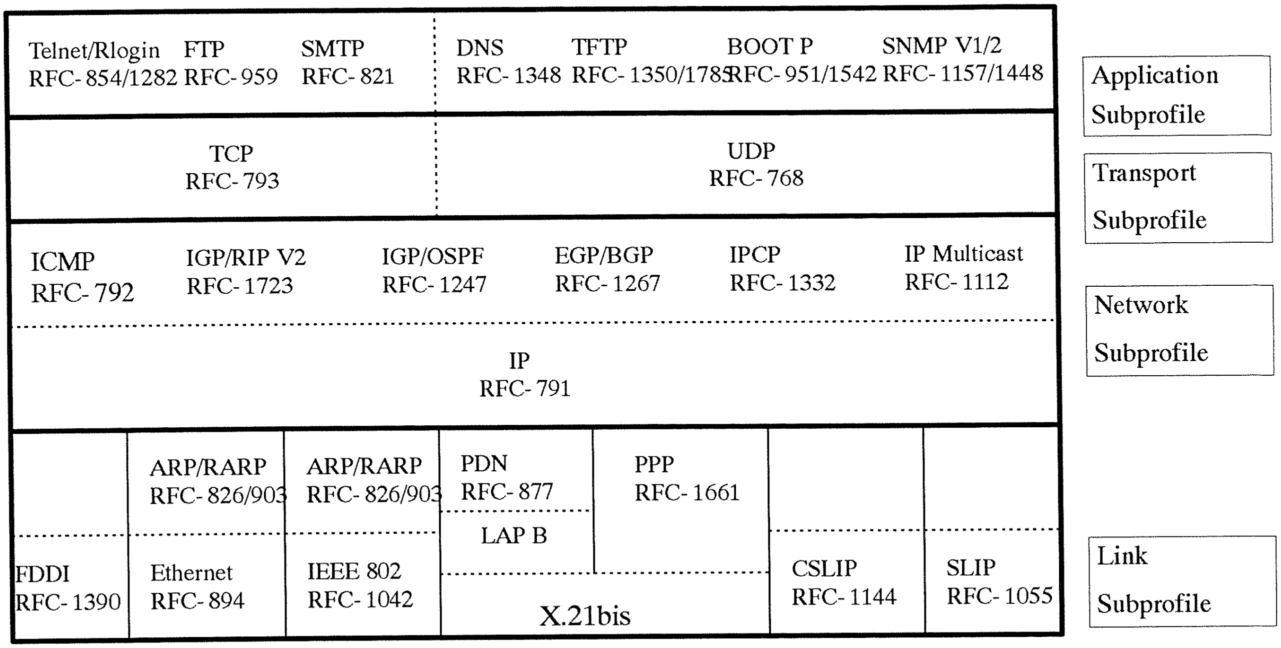

FIGURE 3. Internet protocol suite, protocol stack

The protocols used and the number of layers in the protocol hierarchy are dependent upon the type of services the network will provide to the end user. The individual layer of a protocol stack is referred to as a subprofile. Each subprofile consists of identifying the protocols for a specific layer that will allow the network to provide the desired services. The four IPS subprofile types deployed in FAA networks are: link, network, transport, and user extended, as identified in Figure 4.

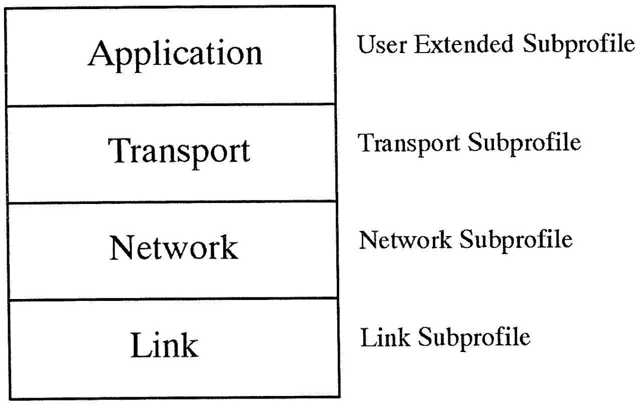

FIGURE 4. Subprofile layers

5.1.1 Link subprofile. The subnetwork subprofile specifies the protocols that provide services corresponding to the physical and data link layers. Users may be directly connected to either the NAS backbone Wide Area Network (WAN) or to a NAS access LAN. Backbone WAN end-systems adhere to the backbone WAN subprofile, which is based on the fiber distributed data interface (FDDI) protocol. Access LAN end-systems adhere to the available access LAN subprofiles, which are based on Ethernet, Token Ring, or serial interface protocols. Access LAN end-systems are connected to backbone WAN and remote LAN end systems via a NAS multiprotocol router. End-systems should implement the backbone WAN subprofile, the Ethernet access LAN subprofile, or the Token Ring access LAN subprofile in accordance with FAA-STD-039B, NAS Open System Architecture and Protocols for the physical link. The link protocols should be implemented in accordance with the specification applicable to the physical interface. Implementation of the Link Subprofile should be done in accordance with RFC-1122, Requirements for Internet Hosts-Communication Layers.

5.1.1.1 LAN connections. The NAS supports the following LAN interfaces.

5.1.1.1.1 Ethernet. Transmission of IP datagrams over Ethernet networks should be in accordance with FAA-STD-039B, NAS Open System Architecture and Protocols and RFC 894, A Standard for the Transmission of IP Datagrams over Ethernet Networks.

5.1.1.1.2 IEEE 802. Transmission of IP datagrams over Institute of Electrical and Electronics Engineers (IEEE) 802 networks should be in accordance with FAA-STD-039B, NAS Open System Architecture and Protocols, and RFC-1042, A Standard for the Transmission of IP Datagrams over IEEE 802 Networks.

5.1.1.1.3 FDDI. Transmission of IP datagrams over FDDI networks should be in accordance with FAA-STD-039B, NAS Open System Architecture and Protocols, and RFC-1390, Transmission of IP and address resolution protocol (ARP) over FDDI Networks.

5.1.1.1.4 ARP/Reverse Address Resolution Protocol (RARP). Implementation of address resolution between the FDDI, Ethernet or IEEE 802 addresses and the IP addresses should be in accordance with RFC-826, Address Resolution Protocol (ARP), or RFC-903, Reverse Address Resolution Protocol (RARP).

5.1.1.2 Serial interfaces. Encapsulation of IP datagrams on serial lines should be performed in accordance with one of the following RFCs:

- RFC-1055, Nonstandard for Transmission of IP Datagrams over Serial Lines: Serial Line Internet Protocol (SLIP),
- RFC-1144, Compressing TCP/IP Headers for Low-speed Serial Links,
- RFC-1661, The Point-to-Point Protocol (PPP).

5.1.1.3 Packet Switched Network (PSN X.25). Implementation of the physical and data link layers of X.25 for an IPS network should be in accordance with FAA-STD-039B, NAS Open System Architecture and Protocols, RFC-1356, Multiprotocol Interconnect on X.25, and ISDN in the Packet Mode.

5.1.1.4 Loopback interface. The link implementation should support a loopback interface that allows a client and server on the same host to communicate with each other using TCP/IP. The class A network ID 127 is reserved for the loopback interface, refer to RFC- 1166, Internet Numbers, for detailed network number information.

5.1.1.5 Maximum Transmission Unit (MTU). The maximum byte size of a frame that can be encapsulated is referred to as the maximum transmission unit (MTU). The MTU for Ethernet is 1500 bytes and the MTU for IEEE 802 is 1492 bytes. The MTU for a point- to- point link (e.g., SLIP or PPP) is determined by the desired response time, refer to RFC- 1191, Path MTU Discovery, for detailed MTU information.

5.1.2 Network subprofile. The network subprofile specifies the protocols that provide services corresponding to the network layer. The protocol used in the IPS networks is IP. IP is designed for use in interconnected packet- switched computer communication networks and provides addressing and fragmentation services. This is not a reliable communication facility. If a higher quality of service is desired, those features must be implemented by a higher layer protocol. Implementation of the network subprofile should be in accordance with RFC- 1122, Requirements for Internet Hosts- Communication Layers.

5.1.2.1 Internet Protocol (IP). IP support should be in accordance with RFC- 791, Internet Protocol.

5.1.2.1.1 Network addressing. Network addressing should be in accordance with Guidance ENET1370- 002.1A, for nonoperational networks, and FAA- STD- 042A, for operational networks.

5.1.2.1.2 Subnet extensions. Subnet extensions to the addressing architecture should be in accordance with RFC- 950, Internet Standard Subnetting Procedure.

5.1.2.1.3 IP multicasting. Multicasting support should be in accordance with RFC- 1112, Internet Group Management Protocol (IGMP).

5.1.2.2 Routing. Networks under the same administrative control are referred to as autonomous systems. Routers used for information exchange within autonomous systems are called interior routers and they use interior gateway protocols (IGP). Routers that move information between autonomous systems are exterior routers and they use exterior gateway protocols (EGP). Dynamic routing for IPS environments should be implemented using either IGP or EGP routers.

5.1.2.2.1 IGP. The IGPs supported by an IPS autonomous router (same network) should be in accordance with either RFC- 1583, Open Shortest Path First (OSPF) V2 or RFC- 1723, Routing Information Protocol (RIP) V2.

5.1.2.2.2 EGP. The EGPs supported by an IPS router that moves information between autonomous systems (different networks) should be in accordance with RFC-1267, Border Gateway Protocol 3 (BGP-3).

5.1.2.2.3 Error detection and reporting. Error detection and reporting should be accomplished using RFC-950, Internet Standard Subnetting Procedure.

5.1.2.3 Network control protocol for PPP. The network control protocol implemented for PPP should be in accordance with RFC-1332, The PPP Internet Protocol Control Protocol (IPCP).

5.1.3 Transport subprofile. The transport subprofile specifies the protocols that provide services for the transport layer of the IPS protocol stack. The IPS transport layer will support two transport subprofiles. The available subprofiles are the IPS connection-oriented (CO) transport subprofile or the IPS connection-less (CL) transport subprofile.

CO service is provided using the TCP, which is the primary virtual-circuit transport protocol for IPS. TCP provides reliable, in-sequence delivery of a full-duplex data stream and is used by applications requiring reliable, CO service (i.e., single mail transfer protocol [SMTP], FTP, Telnet).

CL service is provided using the UDP, which offers minimal transport service and does not provide guaranteed delivery. This protocol gives applications direct access to the datagram service of the IP layer. The only services this protocol provides over IP are checksumming of the data and multiplexing by port number. Therefore, applications running over UDP must deal directly with end-to-end communication problems that a CO protocol would have handled (i.e., transmission for reliable delivery, packetization and reassembly, flow control, etc.). UDP is used by applications that do not require the level of service that TCP provides or if communications services that TCP does not provide (i.e., broadcast, multicast) are to be used.

Implementation of the Transport subprofile should be done in accordance with RFC-1122, Requirements for Internet Hosts-Communication Layers.

5.1.3.1 TCP. The reliable, CO communication protocol used in IPS networks should be TCP. The protocol should be implemented in accordance with RFC-793, Transmission Control Protocol.

5.1.3.2 UDP. The unreliable, CL oriented communication protocol used in IPS networks should be UDP. The protocol should be implemented in accordance with RFC-768, User Datagram Protocol.

5.1.4 User extended subprofile. The user extended subprofile provides services corresponding to the application layer. The applications available are dependent upon the implemented transport layer and end-user requirements.

The user extended subprofile is transport layer specific and cannot be interchanged between the transport subprofiles. Therefore, exercise caution when implementing user extended subprofile. Prior to implementing a user extended subprofile verify that the applicable transport layer is supported by the network.

In order to efficiently use the existing World Wide Web, also known as the Internet, the FAA subnetworks must support the standard application configuration. This will enable subnetworks to connect to the Internet with fewer problems and support the existing services. The current standard Internet services are:

- Remote Login,
- File Transfer,
- Electronic Mail,
- Support Services.

The general implementation of these services should be in accordance with RFC-1123, Requirements for Internet Hosts-Application and Support.

5.1.4.1 Remote login. The standard internet application protocol for remote login is Telnet. It provides the encoding rules necessary to link a user's keyboard/display on a client system with a command interpreter on a remote server system.

5.1.4.1.1 Telnet. Implementation of Telnet should be in accordance with RFC-854, Telnet Protocol Specification.

5.1.4.2 File transfer. The user extended subprofile supports two file transfer protocols, one for TCP and another for UDP. The file transfer protocol for TCP is FTP. The file transfer protocol for UDP is trivial file transfer protocol (TFTP).

5.1.4.2.1 FTP. Implementation of the FTP for TCP should be in accordance with RFC-959, File Transfer Protocol. The file transfer capability of FTP allows a user to copy a file from one system to another system.

5.1.4.2.2 TFTP. Implementation of the file transfer protocol for UDP should be done in accordance with RFC-1782, TFTP Option Extension, RFC-1783, TFTP Blocksize Option, RFC-1784, TFTP Timeout Interval and Transfer Size Options, and RFC-1785, TFTP Option Negotiation Analysis. TFTP is a simple and small file transfer protocol. It is intended to be used when bootstrapping diskless systems (i.e. workstations or X-terminals); therefore, implementations of TFTP can fit in read-only memory.

5.1.4.3 Electronic mail. Mail is sent by a series of request/response transactions between a client, the sender-SMTP, and a server, the receiver-SMTP, using the SMTP.

5.1.4.3.1 SMTP. Implementation of electronic mail for TCP should be in accordance with RFC-821, Simple Mail Transfer Protocol, RFC-1148, Mapping between X.400 (1988)/ ISO 100021, and RFC-822.

5.1.4.4 Support services. The following sections cover the protocols necessary to supply support services. The standard support services are domain name system, host initialization, and network management. Implementation of these services should be in accordance with RFC-1123, Requirements for Internet Hosts-Application and Support.

5.1.4.4.1 Domain name system. A host must implement a resolver to convert host names to IP addresses and vice-versa. Implementation of a domain name system should be in accordance with the following RFCs:

- DOD Internet Host Table Specification (Optional),
- RFC-974, Mail Routing and the Domain System,
- RFC-1101, DNS Encoding of Network Names and Other Types,
- RFC-1183, New DNS RR Definitions,
- RFC-1706, DNS NSAP Resource Records.

5.1.4.4.2 Host initialization. When initializating a diskless host that contains no permanent storage configuration information must be dynamically obtained from the network. Diskless host initialization should be in accordance with the following RFCs:

- RFC-906, Bootstrap Loading Using TFTP,
- RFC-951, Bootstrap Protocol,
- RFC-1084, BootP Vendor Information Extensions.

5.1.4.5 Network management. Network management should be implemented using either simple network management protocol (SNMP) over UDP or common management information protocol (CMIP) over TCP. Therefore, in order to allow management to be performed by either protocol, a host must implement an appropriate management agent for both SNMP and CMIP. Implementation of network management should be in accordance with FAA-HDBK-002, Systems Management.

5.1.4.6 Security. Network security services, which include authentication, encryption, access control, and data integrity, should be in accordance with FAA-STD-045, NAS Network Security Protocols and Mechanisms.

5.1.4.7 Priority. Application priority should be in accordance with FAA-STD-043A, NAS Priority.

5.1.4.8 Interoperability and conformance testing. System and network interoperability and conformance testing should be in accordance with FAA-STD-047, NAS Conformance Testing, and FAA-STD-048, NAS Interoperability Standard.

5.1.4.9 Naming and addressing. System naming and addressing should be in accordance with FAA-STD-042A, Open System Interconnection (OSI) Naming and Addressing.

6. NOTES

6.1 Application program interface. Application programming interfaces (API) define how programmers utilize a particular computer feature. Commonly referred to as sockets, APIs are available for windowing systems, file systems, database systems, and networking systems.

6.1.1 Sockets. A socket is one end of a two-way communications link between two programs running on a network. Sockets are used to implement the connection between a client program and a server program. Mail, FTP, Telnet, name, and finger are all examples of services provided by computers on a network. Typically, each service is provided on a dedicated, well-known port. A program can access a specific service by connecting to the port dedicated to that service. In addition to the ports that are dedicated to specific services, computers also have other ports that let programmers create their own services. Typically ports are numbered and a program connects to a port by specifying the port number of the service. Each service or port recognizes a certain protocol, so requests should be formulated in a manner specific to the desired service. This ensures that a request is understood and a response is received. Port assignments should be in accordance with RFC-1700, Assigned Numbers.

Typically UNIX systems use Berkeley Sockets, System V Transport Layer Interface (TLI), and Remote Procedure Call (RPC) API. Berkeley Sockets and System V TLI provide the same functionality, which is access to TCP and UDP, and are mutually exclusive. However, it is possible to write conditionally-compiled software to support either API. RPC supports network subroutines using Sun's RPC protocol. Microsoft has a sockets-like programming interface, but emphasizes event-based non-blocking to provide constant handling of graphical user interface (GUI) events.

UDP communications requires DGRAM sockets. Once created, a DGRAM socket can immediately be used to transmit UDP packets. TCP requires STREAM sockets, a STREAM socket cannot send or receive data until a connection has been established. Therefore, prior to implementing an application, the applicable socket must be available to support end-to-end communications.

APPENDIX A

PROFILE RECOMMENDATIONS LISTS COMMUNICATIONS LAYERS

A.1 SCOPE

A.1.1 Scope. This appendix contains a summary or the recommendations for the link, network (IP), and transport layers of the IPS. Contained in the summary tables are the feature names, applicable referenced section in RFC- 1122, and implementation conditions.

A.2 APPLICABLE DOCUMENTS

RFC- 1122	Requirements for Internet Hosts- Communication Layers

A.3 DEFINITIONS

A.3.1 Applicable definitions. In addition to the definitions listed in this section, the definitions in Section 3 of this handbook apply to this appendix.

MUST This word or the adjective ”REQUIRED” means that the item is an absolute requirement of the specification.

SHOULD This word or the adjective ”RECOMMENDED” means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

MAY This word or the adjective ”OPTIONAL” means that this item is truly optional. For example; one vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, and another vendor may omit the same item.

A.4 GENERAL RECOMMENDATIONS

A.4.1 General. The tables in this appendix list the features that should be implemented in an IPS network.

TABLE A-I. Link layer conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
Trailer encapsulation	2.3.1			x			
Send Trailers by default without negotiation	2.3.1					x	
ARP	2.3.2						
Flush out-of-date ARP cache entries	2.3.2.1	x					
Prevent ARP floods	2.3.2.1	x					
Cache timeout configurable	2.3.2.1		x				
Save at least one (latest) unresolved pkt	2.3.2.2		x				
Ethernet and IEEE 802 Encapsulation	2.3.3						
Host able to:	2.3.3						
Send & receive RFC-894 encapsulation	2.3.3	x					
Receive RFC-1042 encapsulation	2.3.3		x				
Send RFC-1042 encapsulation	2.3.3			x			
Then config. sw. to select, RFC-894 dflt	2.3.3	x					
Send K1=6 encapsulation	2.3.3					x	
Use ARP on Ethernet and IEEE 802 nets	2.3.3	x					
Link layer report b'casts to IP layer	2.4	x					
IP layer pass TOS to link layer	2.4	x					
No ARP cache entry treated as Dest. Unreach.	2.4					x	

TABLE A-II. Internet protocol layer conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
Implement IP and ICMP	3.1	x					
Handle remote multihoming in application layer	3.1	x					
Support local multihoming	3.1			x			
Meet gateway specs if forward datagrams	3.1	x					
Configuration switch for embedded gateway	3.1	x					1
Config switch default to non-gateway	3.1	x					1
Auto-config based on number of interfaces	3.1					x	1
Able to log discarded datagrams	3.1		x				
Record in counter	3.1		x				
Silently discard Version != 4	3.2.1.1	x					
Verify IP checksum, silently discard bad dgram	3.2.1.2	x					
Addressing:							
Subnet addressing (RFC-950)	3.2.1.3	x					
Src address must be host's own IP address	3.2.1.3	x					
Silently discard datagram with bad dest addr	3.2.1.3	x					
Silently discard datagram with bad src addr	3.2.1.3	x					
Support reassembly	3.2.1.4	x					
Retain same Id field in identical datagram	3.2.1.5			x			
TOS:							
Allow transport layer to set TOS	3.2.1.6	x					
Pass received TOS up to transport layer	3.2.1.6		x				
Use RFC-795 link-layer mappings for TOS	3.2.1.6				x		
TTL:							
Send packet with TTL of 0	3.2.1.7					x	
Discard received packets with TTL < 2	3.2.1.7					x	
Allow transport layer to set TTL	3.2.1.7	x					
Fixed TTL is configurable	3.2.1.7	x					
IP Options:							
Allow transport layer to send IP options	3.2.1.8	x					
Pass all IP options rcvd to higher layer	3.2.1.8	x					
IP layer silently ignore unknown options	3.2.1.8	x					
Security option	3.2.1.8a			x			
Send Stream Identifier option	3.2.1.8b				x		
Silently ignore Stream Identifier option	3.2.1.8b	x					

TABLE A-II. Internet protocol layer conditions summary - Continued

Record Route option	3.2.1.8d			x		
Timestamp option	3.2.1.8e			x		
Source Route (SR) Option:						
Originate & terminate SR options	3.2.1.8c	x				
Datagram with completed SR passed up to TL	3.2.1.8c	x				
Build correct (non-redundant) return route	3.2.1.8c	x				
Send multiple SR options in one header	3.2.1.8c					x
ICMP:						
Silently discard ICMP msg with unknown type	3.2.2	x				
Include more than 8 octets of orig datagram	3.2.2			x		
Included octets same as received	3.2.2	x				
Demux ICMP Error to transport protocol	3.2.2	x				
Send ICMP error message with TOS=0	3.2.2		x			
Send ICMP error message for:						
- ICMP error msg	3.2.2					x
- IP b'cast or IP m'cast	3.2.2					x
- Link-layer b'cast	3.2.2					x
- Non-initial fragment	3.2.2					x
- Datagram with non-unique src address	3.2.2					x
Return ICMP error msgs (when not prohibited)	3.3.8	x				
Dest Unreachable:						
Generate Dest Unreachable (code 2/3)	3.2.2.1		x			
Pass ICMP Dest Unreachable to higher layer	3.2.2.1	x				
Higher layer act on Dest Unreach	3.2.2.1		x			
Interpret Dest Unreach as only hint	3.2.2.1	x				
Redirect:						
Host send Redirect	3.2.2.2				x	
Update route cache when recv Redirect	3.2.2.2	x				
Handle both Host and Net Redirects	3.2.2.2	x				
Discard illegal Redirect	3.2.2.2		x			
Source Quench:						
Send Source Quench if buffering exceeded	3.2.2.3			x		
Pass Source Quench to higher layer	3.2.2.3	x				
Higher layer act on Source Quench	3.2.2.3		x			
Time Exceeded: pass to higher layer	3.2.2.4	x				
Parameter Problem:						
Send Parameter Problem messages	3.2.2.5		x			
Pass Parameter Problem to higher layer	3.2.2.5	x				
Report Parameter Problem to user	3.2.2.5			x		
ICMP Echo Request or Reply:						
Echo server and Echo client	3.2.2.6	x				
Echo client	3.2.2.6		x			
Discard Echo Request to broadcast address	3.2.2.6			x		
Discard Echo Request to multicast address	3.2.2.6			x		
Use specific-dest addr as Echo Reply src	3.2.2.6	x				

TABLE A-II. Internet protocol layer conditions summary - Continued

Send same data in Echo Reply	3.2.2.6	x					
Pass Echo Reply to higher layer	3.2.2.6	x					
Reflect Record Route, Time Stamp options	3.2.2.6		x				
Reverse and reflect Source Route option	3.2.2.6	x					
ICMP Information Request or Reply:	3.2.2.7				x		
ICMP Timestamp (TS) and Timestamp Reply:	3.2.2.8			x			
Minimize delay variability	3.2.2.8		x				1
Silently discard b'cast Timestamp	3.2.2.8			x			1
Silently discard m'cast Timestamp	3.2.2.8			x			1
Use specific-dest addr as TS Reply src	3.2.2.8	x					1
Reflect Record Route, Time Stamp options	3.2.2.6		x				1
Reverse and reflect Source Route option	3.2.2.8	x					1
Pass Timestamp Reply to higher layer	3.2.2.8	x					1
Obey rules for "standard value"	3.2.2.8	x					1
ICMP Address Mask Request and Reply:							
Addr Mask source configurable	3.2.2.9	x					
Support static configuration of addr mask	3.2.2.9	x					
Get addr mask dynamically during booting	3.2.2.9			x			
Get addr via ICMP Addr Mask Request/Reply	3.2.2.9			x			
Retransmit Addr Mask Req if no Reply	3.2.2.9	x					3
Assume default mask if no Reply	3.2.2.9		x				3
Update address mask from first Reply only	3.2.2.9	x					3
Reasonableness check on Addr Mask	3.2.2.9		x				
Send unauthorized Addr Mask Reply msgs	3.2.2.9					x	
Explicitly configured to be agent	3.2.2.9	x					
Static config=> Addr-Mask-Authoritative flag	3.2.2.9		x				
Broadcast Addr Mask Reply when init.	3.2.2.9	x					3
ROUTING OUTBOUND DATAGRAMS:							
Use address mask in local/remote decision	3.3.1.1	x					
Operate with no gateways on conn network	3.3.1.1	x					
Maintain "route cache" of next-hop gateways	3.3.1.2	x					
Treat Host and Net Redirect the same	3.3.1.2		x				
If no cache entry, use default gateway	3.3.1.2	x					
Support multiple default gateways	3.3.1.2	x					
Provide table of static routes	3.3.1.2			x			
Flag: route overridable by Redirects	3.3.1.2			x			
Key route cache on host, not net address	3.3.1.3			x			
Include TOS in route cache	3.3.1.3		x				
Able to detect failure of next-hop gateway	3.3.1.4	x					
Assume route is good forever	3.3.1.4				x		
Ping gateways continuously	3.3.1.4					x	
Ping only when traffic being sent	3.3.1.4	x					
Ping only when no positive indication	3.3.1.4	x					
Higher and lower layers give advice	3.3.1.4		x				

TABLE A-II. Internet protocol layer conditions summary - Continued

Switch from failed default g'way to another	3.3.1.5	x					
Manual method of entering config info	3.3.1.6	x					
REASSEMBLY and FRAGMENTATION:							
Able to reassemble incoming datagrams	3.3.2	x					
At least 576 byte datagrams	3.3.2	x					
EMTU_R configurable or indefinite	3.3.2		x				
Transport layer able to learn MMS_R	3.3.2	x					
Send ICMP Time Exceeded on reassembly timeout	3.3.2	x					
Fixed reassembly timeout value	3.3.2		x				
Pass MMS_S to higher layers	3.3.3	x					
Local fragmentation of outgoing packets	3.3.3			x			
Else don't send bigger than MMS_S	3.3.3	x					
Send max 576 to off-net destination	3.3.3		x				
All-Subnets-MTU configuration flag	3.3.3			x			
MULTIHOMING:							
Reply with same addr as spec-dest addr	3.3.4.2		x				
Allow application to choose local IP addr	3.3.4.2	x					
Silently discard d'gram in "wrong" interface	3.3.4.2			x			
Only send d'gram through "right" interface	3.3.4.2			x			4
SOURCE-ROUTE FORWARDING:							
Forward datagram with Source Route option	3.3.5			x			1
Obey corresponding gateway rules	3.3.5	x					1
Update TTL by gateway rules	3.3.5	x					1
Able to generate ICMP err code 4, 5	3.3.5	x					1
IP src addr not local host	3.3.5			x			1
Update TS, Record Route options	3.3.5	x					1
Configurable switch for non-local SRing	3.3.5	x					1
Defaults to OFF	3.3.5	x					1
Satisfy gwy access rules for non-local SRing	3.3.5	x					1
If not forward, send Dest Unreach (cd 5)	3.3.5		x				2
BROADCAST:							
Broadcast addr as IP source addr	3.2.1.3					x	
Receive 0 or -1 broadcast formats OK	3.3.6		x				
Config'ble option to send 0 or -1 b'cast	3.3.6			x			
Default to -1 broadcast	3.3.6		x				
Recognize all broadcast address formats	3.3.6	x					
Use IP b'cast/m'cast addr in link-layer b'cast	3.3.6	x					
Silently discard link-layer-only b'cast dg's	3.3.6		x				
Use Limited Broadcast addr for connected net	3.3.6		x				
MULTICAST:							
Support local IP multicasting (RFC-1112)	3.3.7		x				
Support IGMP (RFC-1112)	3.3.7			x			

TABLE A-II. Internet protocol layer conditions summary - Concluded

Join all-hosts group at startup	3.3.7		x				
Higher layers learn i'face m'cast capability	3.3.7		x				
INTERFACE:							
Allow transport layer to use all IP mechanisms	3.4	x					
Pass interface ident up to transport layer	3.4	x					
Pass all IP options up to transport layer	3.4	x					
Transport layer can send certain ICMP messages	3.4	x					
Pass spec'd ICMP messages up to transp. layer	3.4	x					
Include IP hdr+8 octets or more from orig.	3.4	x					
Able to leap tall buildings at a single bound	3.5		x				

Footnotes:

(1) Only if feature is implemented.
(2) This condition is overruled if datagram is an ICMP error message.
(3) Only if feature is implemented and is configured "on".
(4) Unless has embedded gateway functionality or is source routed.

TABLE A-III. UDP conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
UDP							
UDP send Port Unreachable	4.1.3.1		x				
IP Options in UDP							
- Pass rcv'd IP options to applic layer	4.1.3.2	x					
- Applic layer can specify IP options in Send	4.1.3.2	x					
- UDP passes IP options down to IP layer	4.1.3.2	x					
Pass ICMP msgs up to applic layer	4.1.3.3	x					
UDP checksums:							
- Able to generate/check checksum	4.1.3.4	x					
- Silently discard bad checksum	4.1.3.4	x					
- Sender Option to not generate checksum	4.1.3.4			x			
- Default is to checksum	4.1.3.4	x					
- Receiver Option to require checksum	4.1.3.4			x			
UDP Multihoming							
- Pass spec-dest addr to application	4.1.3.5	x					
- Applic layer can specify Local IP addr	4.1.3.5	x					
- Applic layer specify wild Local IP addr	4.1.3.5	x					
- Applic layer notified of Local IP addr used	4.1.3.5		x				
Bad IP src addr silently discarded by UDP/IP	4.1.3.6	x					
Only send valid IP source address	4.1.3.6	x					
UDP Application Interface Services							
Full IP interface of 3.4 for application	4.1.4	x					
- Able to spec TTL, TOS, IP opts when send dg	4.1.4	x					
- Pass received TOS up to applic layer	4.1.4			x			

TABLE A-IV. TCP conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
Push flag							
Aggregate or queue un-pushed data	4.2.2.2			x			
Sender collapse successive PSH flags	4.2.2.2		x				
SEND call can specify PUSH	4.2.2.2			x			
If cannot: sender buffer indefinitely	4.2.2.2					x	
If cannot: PSH last segment	4.2.2.2	x					
Notify receiving ALP of PSH	4.2.2.2			x			1
Send max size segment when possible	4.2.2.2		x				
Window							
Treat as unsigned number	4.2.2.3	x					
Handle as 32-bit number	4.2.2.3		x				
Shrink window from right	4.2.2.16				x		
Robust against shrinking window	4.2.2.16	x					
Receiver's window closed indefinitely	4.2.2.17			x			
Sender probe zero window	4.2.2.17	x					
First probe after RTO	4.2.2.17		x				
Exponential backoff	4.2.2.17		x				
Allow window stay zero indefinitely	4.2.2.17	x					
Sender timeout OK conn with zero wind	4.2.2.17					x	
Urgent Data							
Pointer points to last octet	4.2.2.4	x					
Arbitrary length urgent data sequence	4.2.2.4	x					
Inform ALP asynchronously of urgent data	4.2.2.4	x					1
ALP can learn if/how much urgent data Q'd	4.2.2.4	x					1
TCP Options							
Receive TCP option in any segment	4.2.2.5	x					
Ignore unsupported options	4.2.2.5	x					
Cope with illegal option length	4.2.2.5	x					
Implement sending & receiving MSS option	4.2.2.6	x					
Send MSS option unless 536	4.2.2.6		x				
Send MSS option always	4.2.2.6			x			
Send-MSS default is 536	4.2.2.6	x					
Calculate effective send seg size	4.2.2.6	x					
TCP Checksums							

TABLE A-IV. TCP conditions summary - Continued

Sender compute checksum	4.2.2.7	x				
Receiver check checksum	4.2.2.7	x				
Use clock-driven ISN selection	4.2.2.9	x				
Support simultaneous open attempts	4.2.2.10	x				
SYN-RCVD remembers last state	4.2.2.11	x				
Passive Open call interfere with others	4.2.2.18					x
Function: simultan. LISTENs for same port	4.2.2.18	x				
Ask IP for src address for SYN if necc.	4.2.3.7	x				
Otherwise, use local addr of conn.	4.2.3.7	x				
OPEN to broadcast/multicast IP Address	4.2.3.14					x
Silently discard seg to bcast/mcast addr	4.2.3.14	x				
Closing Connections						
RST can contain data	4.2.2.12		x			
Inform application of aborted conn	4.2.2.13	x				
Half-duplex close connections	4.2.2.13			x		
Send RST to indicate data lost	4.2.2.13		x			
In TIME-WAIT state for 2xMSL seconds	4.2.2.13	x				
Accept SYN from TIME-WAIT state	4.2.2.13			x		
Retransmissions						
Jacobson Slow Start algorithm	4.2.2.15	x				
Jacobson Congestion-Avoidance algorithm	4.2.2.15	x				
Retransmit with same IP ident	4.2.2.15			x		
Karn's algorithm	4.2.3.1	x				
Jacobson's RTO estimation alg.	4.2.3.1	x				
Exponential backoff	4.2.3.1	x				
SYN RTO calc same as data	4.2.3.1		x			
Recommended initial values and bounds	4.2.3.1		x			
Generating ACK's:						
Queue out-of-order segments	4.2.2.20		x			
Process all Q'd before send ACK	4.2.2.20	x				
Send ACK for out-of-order segment	4.2.2.21			x		
Delayed ACK's	4.2.3.2		x			
Delay < 0.5 seconds	4.2.3.2	x				
Every 2nd full-sized segment ACK'd	4.2.3.2	x				
Receiver SWS-Avoidance Algorithm	4.2.3.3	x				
Sending data						
Configurable TTL	4.2.2.19	x				
Sender SWS-Avoidance Algorithm	4.2.3.4	x				
Nagle algorithm	4.2.3.4		x			
Application can disable Nagle algorithm	4.2.3.4	x				
Connection Failures:						
Negative advice to IP on R1 retxs	4.2.3.5	x				

TABLE A-IV. TCP conditions summary - Concluded

Close connection on R2 retxs	4.2.3.5	x					
ALP can set R2	4.2.3.5	x					1
Inform ALP of R1<=retxs<R2	4.2.3.5		x				1
Recommended values for R1, R2	4.2.3.5		x				
Same mechanism for SYNs	4.2.3.5	x					
R2 at least 3 minutes for SYN	4.2.3.5	x					
Send Keep-alive Packets:	4.2.3.6			x			
- Application can request	4.2.3.6	x					
- Default is "off"	4.2.3.6	x					
- Only send if idle for interval	4.2.3.6	x					
- Interval configurable	4.2.3.6	x					
- Default at least 2 hrs.	4.2.3.6	x					
- Tolerant of lost ACK's	4.2.3.6	x					
IP Options							
Ignore options TCP doesn't understand	4.2.3.8	x					
Time Stamp support	4.2.3.8			x			
Record Route support	4.2.3.8			x			
Source Route:							
ALP can specify	4.2.3.8	x					1
Overrides src rt in datagram	4.2.3.8	x					
Build return route from src rt	4.2.3.8	x					
Later src route overrides	4.2.3.8		x				
Receiving ICMP Messages from IP	4.2.3.9	x					
Dest. Unreach (0,1,5) => inform ALP	4.2.3.9		x				
Dest. Unreach (0,1,5) => abort conn	4.2.3.9					x	
Dest. Unreach (2-4) => abort conn	4.2.3.9		x				
Source Quench => slow start	4.2.3.9		x				
Time Exceeded => tell ALP, don't abort	4.2.3.9		x				
Param Problem => tell ALP, don't abort	4.2.3.9		x				
Address Validation							
Reject OPEN call to invalid IP address	4.2.3.10	x					
Reject SYN from invalid IP address	4.2.3.10	x					
Silently discard SYN to bcast/mcast addr	4.2.3.10	x					
TCP/ALP Interface Services							
Error Report mechanism	4.2.4.1	x					
ALP can disable Error Report Routine	4.2.4.1		x				
ALP can specify TOS for sending	4.2.4.2	x					
Passed unchanged to IP	4.2.4.2		x				
ALP can change TOS during connection	4.2.4.2		x				
Pass received TOS up to ALP	4.2.4.2			x			
FLUSH call	4.2.4.3			x			
Optional local IP addr parm. in OPEN	4.2.4.4	x					

FOOTNOTES:

(1) "ALP" means Application-Layer program.

APPENDIX B

PROFILE RECOMMENDATIONS LISTS APPLICATION LAYER

B.1 SCOPE

B.1.1 Scope. This appendix contains a summary or the recommendations for the application layer of the IPS. Contained in the summary tables are the feature names, applicable referenced section in RFC-1123, and implementation conditions.

B.2 APPLICABLE DOCUMENTS

RFC-959	File Transfer Protocol
RFC-1123	Requirements for Internet Hosts-Application and Support

B.3 DEFINITIONS

B.3.1 Applicable definitions. In addition to the definitions listed in this section, the definitions in Section 3 of this handbook apply to this appendix.

MUST This word or the adjective "REQUIRED" means that the item is an absolute requirement of the specification.

SHOULD This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

MAY This word or the adjective "OPTIONAL" means that this item is truly optional. For example; one vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, and another vendor may omit the same item.

B.4 GENERAL RECOMMENDATIONS

B.4.1 General. The tables in this appendix list the features that should be implemented in an IPS network.

TABLE B-I. General application conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
User interfaces:							
Allow host name to begin with digit	2.1	x					
Host names of up to 635 characters	2.1	x					
Host names of up to 255 characters	2.1		x				
Support dotted-decimal host numbers	2.1		x				
Check syntactically for dotted-dec first	2.1		x				
Map domain names per Section 6.1	2.2	x					
Cope with soft DNS errors	2.2	x					
Reasonable interval between retries	2.2	x					
Allow for long outages	2.2	x					
Expect WKS records to be available	2.2				x		
Try multiple addr's for remote multihomed host	2.3		x				
UDP reply src addr is specific dest of request	2.3		x				
Use same IP addr for related TCP connections	2.3		x				
Specify appropriate TOS values	2.4	x					
TOS values configurable	2.4	x					
Unused TOS bits zero	2.4	x					

TABLE B-II. Telnet conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
Option Negotiation	3.2.1	x					
Avoid negotiation loops	3.2.1	x					
Refuse unsupported options	3.2.1	x					
Negotiation OK anytime on connection	3.2.1		x				
Default to NVT	3.2.1	x					
Send official name in Term-Type option	3.2.8	x					
Accept any name in Term-Type option	3.2.8	x					
Implement Binary, Suppress-GA options	3.3.3	x					
Echo, Status, EOL, Ext-Opt-List options	3.3.3		x				
Implement Window-Size option if appropriate	3.3.3		x				
Server initiate mode negotiations	3.3.4		x				
User can enable/disable init negotiations	3.3.4		x				
Go-Aheads							
Non-GA server negotiate SUPPRESS-GA option	3.2.2	x					
User or Server accept SUPPRESS-GA option	3.2.2	x					
User Telnet ignore GA's	3.2.2			x			
Control Functions							
Support SE NOP DM IP AO AYT SB	3.2.3	x					
Support EOR EC EL Break	3.2.3			x			
Ignore unsupported control functions	3.2.3	x					
User, Server discard urgent data up to DM	3.2.4	x					
User Telnet send "Synch" after IP, AO, AYT	3.2.4		x				
Server Telnet reply Synch to IP	3.2.4			x			
Server Telnet reply Synch to AO	3.2.4	x					
User Telnet can flush output when send IP	3.2.4		x				
Encoding							
Send high-order bit in NVT mode	3.2.5				x		
Send high-order bit as parity bit	3.2.5					x	
Negot. BINARY if pass high-ord. bit to applic	3.2.5		x				
Always double IAC data byte	3.2.6	x					
Double IAC data byte in binary mode	3.2.7	x					

TABLE B-II. Telnet conditions summary - concluded

End-of-line, CR NUL in binary mode	3.2.7					x
End-of-Line						
EOL at Server same as local end-of-line	3.3.1	x				
ASCII Server accept CR LF or CR NUL for EOL	3.3.1	x				
User Telnet able to send CR LF, CR NUL, or LF	3.3.1	x				
ASCII user able to select CR LF/CR NUL	3.3.1		x			
User Telnet default mode is CR LF	3.3.1		x			
Non-interactive uses CR LF for EOL	3.3.1	x				
User Telnet interface						
Input & output all 7-bit characters	3.4.1		x			
Bypass local op sys interpretation	3.4.1		x			
Escape character	3.4.1	x				
User-settable escape character	3.4.1		x			
Escape to enter 8-bit values	3.4.1			x		
Can input IP, AO, AYT	3.4.2	x				
Can input EC, EL, Break	3.4.2		x			
Report TCP connection errors to user	3.4.3		x			
Optional non-default contact port	3.4.4		x			
Can spec: output flushed when IP sent	3.4.5		x			
Can manually restore output mode	3.4.5		x			

TABLE B-III. FTP conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
Implement TYPE T if same as TYPE N	4.1.2.2		x				
File/Record transform invertible if poss.	4.1.2.4		x				
User-FTP send PORT cmd for stream mode	4.1.2.5		x				
Server-FTP implement PASV	4.1.2.6	x					
PASV is per-transfer	4.1.2.6	x					
NLST reply usable in RETR cmds	4.1.2.7	x					
Implied type for LIST and NLST	4.1.2.7		x				
SITE cmd for non-standard features	4.1.2.8		x				
STOU cmd return pathname as specified	4.1.2.9	x					
Use TCP READ boundaries on control conn.	4.1.2.10					x	
Server-FTP send only correct reply format	4.1.2.11	x					
Server-FTP use defined reply code if poss.	4.1.2.11		x				
New reply code following Section 4.2	4.1.2.11			x			
User-FTP use only high digit of reply	4.1.2.11		x				
User-FTP handle multi-line reply lines	4.1.2.11	x					
User-FTP handle 421 reply specially	4.1.2.11				x		
Default data port same IP addr as ctl conn	4.1.2.12	x					
User-FTP send Telnet cmds exc. SYNCH, IP	4.1.2.12					x	
User-FTP negotiate Telnet options	4.1.2.12					x	
Server-FTP handle Telnet options	4.1.2.12	x					
Handle ”Experimental” directory cmds	4.1.3.1		x				
Idle timeout in server-FTP	4.1.3.2		x				
Configurable idle timeout	4.1.3.2		x				
Receiver checkpoint data at Restart Marker	4.1.3.4		x				
Sender assume 110 replies are synchronous	4.1.3.4					x	
Support TYPE:							
ASCII - Non-Print (AN)	4.1.2.13	x					
ASCII - Telnet (AT) -- if same as AN	4.1.2.2		x				
ASCII - Carriage Control (AC)	959 3.1.1.5.2			x			
EBCDIC - (any form)	959 3.1.1.2			x			
IMAGE	4.1.2.1	x					
LOCAL 8	4.1.2.1	x					
LOCAL m	4.1.2.1			x			2
Support MODE:							
Stream	4.1.2.13	x					

TABLE B-III. FTP conditions summary - Continued

Block	959 3.4.2			x			
Support STRUCTURE:							
File	4.1.2.13	x					
Record	4.1.2.13	x					3
Page	4.1.2.3				x		
Support commands:							
USER	4.1.2.13	x					
PASS	4.1.2.13	x					
ACCT	4.1.2.13	x					
CWD	4.1.2.13	x					
CDUP	4.1.2.13	x					
SMNT	959 5.3.1			x			
REIN	959 5.3.1			x			
QUIT	4.1.2.13	x					
PORT	4.1.2.13	x					
PASV	4.1.2.6	x					
TYPE	4.1.2.13	x					1
STRU	4.1.2.13	x					1
MODE	4.1.2.13	x					1
RETR	4.1.2.13	x					
STOR	4.1.2.13	x					
STOU	959 5.3.1			x			
APPE	4.1.2.13	x					
ALLO	959 5.3.1			x			
REST	959 5.3.1			x			
RNFR	4.1.2.13	x					
RNTO	4.1.2.13	x					
ABOR	959 5.3.1			x			
DELE	4.1.2.13	x					
RMD	4.1.2.13	x					
MKD	4.1.2.13	x					
PWD	4.1.2.13	x					
LIST	4.1.2.13	x					
NLST	4.1.2.13	x					
SITE	4.1.2.8			x			
STAT	4.1.2.13	x					
SYST	4.1.2.13	x					
HELP	4.1.2.13	x					
NOOP	4.1.2.13	x					
User Interface:							
Arbitrary pathnames	4.1.4.1	x					
Implement "QUOTE" command	4.1.4.2	x					
Transfer control commands immediately	4.1.4.2		x				
Display error messages to user	4.1.4.3		x				
Verbose mode	4.1.4.3		x				
Maintain synchronization with server	4.1.4.4		x				

TABLE B-III. FTP conditions summary - Concluded

Footnotes:

(1) For the values shown earlier.
(2) Here m is number of bits in a memory word.
(3) Required for host with record-structured file system, optional otherwise.

TABLE B-IV. TFTP conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
Fix Sorcerer's Apprentice Syndrome	4.2.3.1	x					
Transfer modes:							
netascii	RFC-783	x					
octet	RFC-783	x					
mail	4.2.2.1				x		
extensions	4.2.3.3			x			
Use adaptive timeout	4.2.3.2	x					
Configurable access control	4.2.3.4		x				
Silently ignore broadcast request	4.2.3.5		x				

TABLE B-V. SMTP conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
RECEIVER-SMTP:							
Implement VRFY	5.2.3	x					
Implement EXPN	5.2.3		x				
EXPN, VRFY configurable	5.2.3			x			
Implement SEND, SOML, SAML	5.2.4			x			
Verify HELO parameter	5.2.5			x			
Refuse message with bad HELO	5.2.5					x	
Accept explicit src-route syntax in env.	5.2.6	x					
Support "postmaster"	5.2.7	x					
Process RCPT when received (except lists)	5.2.7			x			
Long delay of RCPT responses	5.2.7					x	
Add Received: line	5.2.8	x					
Received: line include domain literal	5.2.8		x				
Change previous Received: line	5.2.8					x	
Pass Return-Path info (final deliv/gwy)	5.2.8	x					
Support empty reverse path	5.2.9	x					
Send only official reply codes	5.2.10		x				
Send text from RFC-821 when appropriate	5.2.10		x				
Delete "." for transparency	5.2.11	x					
Accept and recognize self domain literal(s)	5.2.17	x					
Error message about error message	5.3.1					x	
Keep pending listen on SMTP port	5.3.1.2		x				
Provide limit on recv concurrency	5.3.1.2			x			
Wait at least 5 mins for next sender cmd	5.3.2		x				
Avoidable delivery failure after "250 OK"	5.3.3					x	
Send error notification msg after accept	5.3.3	x					
Send using null return path	5.3.3	x					
Send to envelope return path	5.3.3		x				
Send to null address	5.3.3					x	
Strip off explicit src route	5.3.3		x				
Minimize acceptance delay (RFC-1047)	5.3.3	x					
SENDER-SMTP:							
Canonicalized domain names in MAIL, RCPT	5.2.2	x					
Implement SEND, SOML, SAML	5.2.4			x			
Send valid principal host name in HELO	5.2.5	x					

TABLE B-V. SMTP conditions summary - Continued

Send explicit source route in RCPT TO:	5.2.6				x	
Use only reply code to determine action	5.2.10	x				
Use only high digit of reply code when poss.	5.2.10		x			
Add "." for transparency	5.2.11	x				
Retry messages after soft failure	5.3.1.1	x				
Delay before retry	5.3.1.1	x				
Configurable retry parameters	5.3.1.1	x				
Retry once per each queued dest host	5.3.1.1		x			
Multiple RCPT's for same DATA	5.3.1.1		x			
Support multiple concurrent transactions	5.3.1.1			x		
Provide limit on concurrency	5.3.1.1		x			
Timeouts on all activities	5.3.1	x				
Per-command timeouts	5.3.2		x			
Timeouts easily reconfigurable	5.3.2		x			
Recommended times	5.3.2		x			
Try alternate addr's in order	5.3.4	x				
Configurable limit on alternate tries	5.3.4			x		
Try at least two alternates	5.3.4		x			
Load-split across equal MX alternates	5.3.4		x			
Use the Domain Name System	5.3.5	x				
Support MX records	5.3.5	x				
Use WKS records in MX processing	5.2.12				x	
MAIL FORWARDING:						
Alter existing header field(s)	5.2.6				x	
Implement relay function: 821/section 3.6	5.2.6			x		
If not, deliver to RHS domain	5.2.6		x			
Interpret 'local-part' of addr	5.2.16					x
MAILING LISTS AND ALIASES						
Support both	5.3.6		x			
Report mail list error to local admin.	5.3.6	x				
MAIL GATEWAYS:						
Embed foreign mail route in local-part	5.2.16			x		
Rewrite header fields when necessary	5.3.7			x		
Prepend Received: line	5.3.7	x				
Change existing Received: line	5.3.7					x
Accept full RFC-822 on Internet side	5.3.7		x			
Act on RFC-822 explicit source route	5.3.7			x		
Send only valid RFC-822 on Internet side	5.3.7	x				
Deliver error msgs to envelope addr	5.3.7		x			
Set env return path from err return addr	5.3.7		x			
USER AGENT -- RFC-822						
Allow user to enter <route> address	5.2.6				x	
Support RFC-1049 Content Type field	5.2.13			x		
Use 4-digit years	5.2.14		x			

TABLE B-V. SMTP conditions summary - Concluded

Generate numeric timezones	5.2.14		x				
Accept all timezones	5.2.14	x					
Use non-num timezones from RFC-822	5.2.14	x					
Omit phrase before route-addr	5.2.15			x			
Accept and parse dot.dec. domain literals	5.2.17	x					
Accept all RFC-822 address formats	5.2.18	x					
Generate invalid RFC-822 address format	5.2.18					x	
Fully-qualified domain names in header	5.2.18	x					
Create explicit src route in header	5.2.19				x		
Accept explicit src route in header	5.2.19	x					
Send/recv at least 64KB messages	5.3.8	x					

TABLE B-VI. Domain name system conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
GENERAL ISSUES							
Implement DNS name-to-address conversion	6.1.1	x					
Implement DNS address-to-name conversion	6.1.1	x					
Support conversions using host table	6.1.1			x			
Properly handle RR with zero TTL	6.1.2.1	x					
Use QCLASS=* unnecessarily	6.1.2.2		x				
Use QCLASS=IN for Internet class	6.1.2.2	x					
Unused fields zero	6.1.2.3	x					
Use compression in responses	6.1.2.4	x					
Include config info in responses	6.1.2.5					x	
Support all well-known, class-indep. types	6.1.3.5	x					
Easily expand type list	6.1.3.5		x				
Load all RR types (except MD and MF)	6.1.3.6	x					
Load MD or MF type	6.1.3.6					x	
Operate when root servers, etc. unavailable	6.1.3.7	x					
RESOLVER ISSUES:							
Resolver support multiple concurrent requests	6.1.3.1		x				

TABLE B-VI. Domain name system conditions summary - Continued

Full-service resolver:	6.1.3.1			x			
Local caching	6.1.3.1	x					
Information in local cache times out	6.1.3.1	x					
Configurable with starting info	6.1.3.1		x				
Stub resolver:	6.1.3.1			x			
Use redundant recursive name servers	6.1.3.1	x					
Local caching	6.1.3.1			x			
Information in local cache times out	6.1.3.1	x					
Support for remote multi-homed hosts:							
Sort multiple addresses by preference list	6.1.3.4		x				
TRANSPORT PROTOCOLS:							
Support UDP queries	6.1.3.2	x					
Support TCP queries	6.1.3.2		x				
Send query using UDP first	6.1.3.2	x					1
Try TCP if UDP answers are truncated	6.1.3.2		x				
Name server limit TCP query resources	6.1.3.2			x			
Punish unnecessary TCP query	6.1.3.2				x		
Use truncated data as if it were not	6.1.3.2					x	
Private agreement to use only TCP	6.1.3.2			x			
Use TCP for zone transfers	6.1.3.2	x					
TCP usage not block UDP queries	6.1.3.2	x					
Support broadcast or multicast queries	6.1.3.2			x			
RD bit set in query	6.1.3.2					x	
RD bit ignored by server is b'cast/m'cast	6.1.3.2	x					
Send only as occasional probe for addr's	6.1.3.2		x				
RESOURCE USAGE:							
Transmission controls, per [DNS:2]	6.1.3.3	x					
Finite bounds per request	6.1.3.3	x					
Failure after retries => soft error	6.1.3.3	x					
Cache temporary failures	6.1.3.3		x				
Cache negative responses	6.1.3.3		x				
Retries use exponential backoff	6.1.3.3		x				
Upper, lower bounds	6.1.3.3		x				
Client handle Source Quench	6.1.3.3		x				
Server ignore Source Quench	6.1.3.3			x			
USER INTERFACE:							
All programs have access to DNS interface	6.1.4.2	x					
Able to request all info for given name	6.1.4.2	x					
Returns complete info or error	6.1.4.2	x					
Special interfaces	6.1.4.2			x			
Name<->Address translation	6.1.4.2	x					

TABLE B-VI. Domain name system conditions summary - Concluded

Abbreviation Facilities:	6.1.4.3			x			
Convention for complete names	6.1.4.3	x					
Conversion exactly once	6.1.4.3	x					
Conversion in proper context	6.1.4.3	x					
Search list:	6.1.4.3			x			
Administrator can disable	6.1.4.3		x				
Prevention of excessive root queries	6.1.4.3	x					
Both methods	6.1.4.3		x				

1. Unless there is private agreement between particular resolver and particular server.

TABLE B-VII. Management conditions summary

FEATURE	SECTION	MUST	SHOULD	MAY	SHOULD NOT	MUST NOT	Footnotes
Support SNMP or CMOT agent	6.3.1		x				
Implement specified objects in standard MIB	6.3.1		x				